大華建設股份有限公司
資訊安全政策及管理方案

一、資訊安全風險架構

本公司資訊安全之權責單位為管理部所轄之資訊組，於 112 年 10 月 27 日配置專責主管及專責人員各一名，負責統籌資訊安全及相關事宜，並定期進行內部資訊安全檢查及人員資訊安全宣導。

114 年無重大資訊安全事件發生，報告 114/11/12 董事會。

二、資訊安全政策

（一）目的

為強化資訊安全管理，確保資訊資產的機密性、完整性及可用性，以維護資訊系統正常運作，特制定此資訊安全管理政策。

（二）範圍

維持本公司資訊作業正常運作之環境、硬體、軟體、資料及人員。

（三）目標

避免資訊系統遭受來自內、外部人員不當使用或蓄意破壞、或當已遭受不當使用、蓄意破壞等緊急事故時，能迅速應變處置，並在最短時間內回復正常運作，降低該事故可能帶來之公司損失及營運風險。

三、資訊安全管理措施

本公司尚未投保資安險，相關具體預防措施如下：

（一）網路安全管理：

1.為確保公司資訊安全，設置防火牆，隔絕網路病毒、防止入侵攻擊、阻擋惡意連線及上網內容過濾避免進入惡意網站。

2.各辦公室連線公司使用應用系統以 VPN 方式連線，避免資料傳輸過程中遭到非法擷取。

（二）系統存取控制：

1.公司內各應用系統的使用，皆透過程式授權書申請，經權責主管核准後，由資訊組建立帳號並依據程式授權書所申請的功能開放權限。

2.人員職務異動或離職時，須會辦資訊組人員，進行各系統權限修正或刪除帳號。

3.每年列印各使用者權限明細表交由各使用單位審查其系統使用權限與職責相符。

（三）病毒防護與管理：

1.伺服器與各單位電腦設備皆安裝防護軟體，不可任意關閉或移除，防毒軟體病毒碼自動更新，確保能阻擋最新型電腦病毒。

2.電子郵件服務提供信件掃毒功能及信件過濾功能，防堵病毒或垃圾郵件進入使用者電腦。

（四）確保系統的永續運作：

1.目前已進行異地備份作業，以確保資料的安全與完整性。每日透過連線備份至合作廠商的機房進行數據回存，該機房配有不斷電系統，能有效保障資料在異常情況下的完整性。

2.系統發生異常事件無法運作時，依系統復原程序將系統回復正常運作。

（五）電腦設備安全管理：

1.電腦主機，各應用伺服器等設備設置於專用機房內，機房門禁由資訊組人員負責管理，非權責人員進出時須資訊組人員陪同。

2.機房內有獨立空調，以維持電腦設備於適合的溫度環境下運轉。

3.機房內配置不斷電系統以確保供電穩定，以防設備受損造成電腦應用系統無法運作。

（六）企業入口網站導入：

企業入口網站（EIP）及電子簽核系統（BPM）已於 114 年度正式上線並正常運作。EIP 系統統一公司內部資訊存儲與傳遞，透過電子簽核流程取代傳統紙本簽核，達成無紙化與高效率的作業目標。

1. 加強資訊傳遞及外洩防範：
   系統採集中化管理，僅授權人員得以存取，顯著降低資料外洩風險。
2. 資訊安全與合規：
   系統具備簽核、權限管理及操作紀錄等功能，確保文件真實性與安全性。
3. 流程透明化與操作追溯：
   整合審核流程，使簽核歷程清晰可追溯，管理層能即時掌握簽核進度與異常情況。
4. 執行情形：
   企業入口網站及電子簽核系統已正式並正常上線，員工均依相關作業規範執行簽核作業，系統運作穩定，達成預期效益。

（七）Active Directory（AD）帳號控管：

所有公司電腦均已納入 Active Directory（AD）帳號控管，進一步強化內部資訊安全與操作規範，確保公司資料資產安全。

1. 集中化管理：
   透過 AD 系統統一管理全公司員工帳號與密碼，管理層可即時設定與調整使用者權限，確保帳號使用符合工作需求並維持最新狀態。
2. 提升資料安全：
   所有電腦皆經 AD 系統身份驗證與授權，未經授權帳號無法登入公司電腦，有效防止非公司人員的非法使用，降低外部入侵風險。
3. 執行情形：
   新購電腦已全部納入 AD 系統控管，帳號建置及整合運作順利，系統運作穩定，達成集中化與安全化管理目標。

（八）異地備份：

為確保公司關鍵資料在突發事件發生時仍能安全保存並迅速恢復運作，本年度持續執行異地備份作業與定期回存確認。

1. 年度資料回存確認：

   預計每年均進行資料回存確認作業，113 年度（11 月 20 日）之回存測試已順利完成，備份資料完整無誤。

   114 年度資料回存確認預計於 11 月 20 日執行，將於測試機檢查備份資料完整性，以確保公司在發生意外或災害時能持續穩定運行。

2. 執行情形：

   異地備份內部會議 1 次：討論異地備份作業流程與應急演練強化方案，確保資料安全儲存與復原能力完善。

   異地備份外部會議 1 次：與備份合作廠商確認資料傳輸穩定性及不斷電服務系統（UPS）之執行方式。

（九）電腦資產與軟體授權盤點：

為維護公司資訊資產安全及確保軟體使用之合法性，本年度依公司規定持續執行電腦資產與軟體授權盤點作業。

1. 定期盤點作業：

   公司每年定期進行電腦資產與軟體盤點，以確保所有設備及軟體均符合法律及內部資訊安全規範。

2. 114 年度盤點作業：

   (1)依據公司規定，員工於執行職務時禁止使用未合法授權軟體，故於 114 年 7 月 17 日至 8 月 26 日 進行工地電腦軟體盤查作業。

   (2)本次盤查範圍包含工地使用之桌上型電腦及筆記型電腦，共計 68 台。

   (3)盤查項目涵蓋工作相關軟體，如 Windows、Office、AutoCAD、SketchUp 等。

   (4)盤查結果顯示，所有電腦安裝之軟體皆為合法授權版本，無違規情事。

（十）資訊安全宣導：

為提升全體員工之資安意識及防護能力，公司持續推動資訊安全教育與宣導，確保各單位皆能遵守資訊安全規範，降低潛在風險。

1. 定期宣導機制：

   每季均定期舉辦資訊安全宣導，內容涵蓋密碼管理、防範釣魚郵件、機敏資料保護、社交工程防範及行動裝置安全等主題。

2. 推行成效：

   透過持續宣導與案例分享，員工對資訊安全事件的警覺度顯著提升，能主動遵守公司安全政策，有效降低資訊外洩與操作疏失風險。